IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

BLIX INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 19-_____
	)	
APPLE INC.,	)	**JURY TRIAL DEMANDED**
	)	
Defendant.	)	

COMPLAINT

Plaintiff Blix Inc. ("Blix" or "Plaintiff") hereby demands a jury trial and alleges the following against Defendant Apple Inc. ("Apple" or "Defendant"):

INTRODUCTION

1. Plaintiff Blix Inc. is an industry-leading provider of software solutions and innovating messaging products. Ben Volach, co-founder of Blix, has been a pioneer in online messaging for almost 20 years. In 1999 Mr. Volach co-founded Followap—a leading provider of mobile messaging products. Followap enabled advanced interoperable mobile messaging products and presence-enhanced services. It eventually served more than 200 million subscribers before being acquired by NewStar for roughly $140 million.

2. After Followap's success Mr. Volach continued to develop innovative messaging products. Mr. Volach knew that as electronic communication became more prevalent, privacy would become a growing concern. Mr. Volach had a vision for an easy-to-use communication system that would give individuals manageable addresses to control their privacy and manage interactions. Using Mr. Volach's ideas, companies and individuals could use manageable *public* addresses while keeping their *private* address information private. The system Mr. Volach

envisioned was a revolutionary step forward, allowing electronic communication without widespread dissemination of private address information.

3. Mr. Volach captured his vision in a patent application, and the U.S. Patent and Trademark Office ("USPTO") agreed Mr. Volach's ideas were patentable innovations. Mr. Volach received U.S. Patent No. 9,749,284 ("the '284 patent") on August 29, 2017.

4. Mr. Volach used these ideas to develop BlueMail—a beautifully designed, universal email application capable of managing an unlimited number of mail accounts from various providers while enabling personalization across multiple email accounts.

5. BlueMail was first released in 2014 and quickly achieved success on multiple platforms. It became one of the top three email applications on Android, with over one million downloads and more than 500,000 ratings and reviews (91% of which are "highly satisfied"). It achieved similar success on the iOS "App Store." BlueMail was named as one of the "Coolest Must Have Phone Apps" for 2017 by NBC's Today Show.

6. In August 2018, Mr. Volach added innovative anonymous messaging features to BlueMail, adding a "Share Email" feature to facilitate private and easy-to-manage communications options. BlueMail's new "Share Email" feature allows parties to communicate using manageable *public* interaction addresses, without revealing their *private* interaction addresses. This new feature was a major step towards implementing the visionary ideas in Mr. Volach's patent.

7. Not long after Mr. Volach's team unveiled BlueMail's innovative anonymous communication options, Apple took Mr. Volach's pioneering ideas—without permission, payment, or credit—and used those ideas in Apple's own products.

8. In June 2019 Apple announced a new "Sign In With Apple" service for fast, easy-to-use, private messaging. At a worldwide conference for Apple software developers, Apple's Senior Vice President of Software Engineering Craig Federighi described a system for controlled interactions, using manageable public interaction addresses and private interaction addresses. This new system received thunderous applause. But during the presentation, Apple never acknowledged that this idea for manageable interaction addresses was *already* being used in other software—Mr. Volach's popular BlueMail software.

9. Not only did Apple steal BlueMail's pioneering anonymous messaging capabilities—days later, Apple *removed* BlueMail from the MacOS App Store, to prevent Mr. Volach's software from readily reaching consumers and competing with Apple's own products. This unlawfully leveraged Apple's monopoly over MacOS's App Store (Apple's closed system for MacOS application distribution) to extend, maintain, and protect from competition Apple's monopoly power in the market for MacOS mail clients (including Apple's pre-installation of its own proprietary Apple Mail software on each MacOS device Apple sells).

10. Apple's theft of Mr. Volach's patented ideas, days before Apple threw Mr. Volach's very successful software product out of Apple's "App Store" marketplace, caused tremendous harm to Blix. For years Mr. Volach has been preparing to release software that extends BlueMail's use of secure and private messaging, to make full use of Mr. Volach's vision in his '284 patent. For that reason, Mr. Volach co-founded Blix—a successor company to BlueMail—to take the next step in BlueMail's evolution. But Apple's theft of Mr. Volach's patented technology is now crippling the long-planned rollout of new features in BlueMail and Blix.

11. Apple's unexplained refusal to give consumers access to competing software products in the App Store is a threat to Blix's success. The BlueMail client for Mac has been ejected from the App Store, making it inaccessible to consumers who use MacOS and who would benefit from BlueMail's innovative features. Apple's conduct leaves consumers with fewer choices when selecting an email application for MacOS.

12. Consumers also suffer from Apple's pattern of stealing great ideas Apple sees in the App Store. Apple frequently takes other companies' innovative features, adds those ideas to Apple's own software products without permission, and then either ejects the original third-party application from the App Store (as it did with Blix) or causes the third-party software developer to close its doors entirely. This pattern of behavior is well documented. *See, e.g.,* Washington Post, HOW APPLE USES ITS APP STORE TO COPY THE BEST IDEAS (Sept. 15, 2019) (attached as Ex 1) ("Developers have come to accept that, without warning, Apple can make their work obsolete by announcing a new app or feature that uses or incorporates their ideas. Some apps have simply buckled under the pressure, in some cases shutting down. They generally don't sue Apple because of the difficulty and expense in fighting the tech giant—and the consequences they might face from being dependent on the platform… Apple's creation of apps imitating ones that already exist on its platform, aided by market data it collects from them, could be harming competition and hurting innovation.").

13. Blix, and its BlueMail product, are the latest in Apple's long line of victims. Apple's pattern of stealing ideas from the App Store harms software developers and consumers in multiple ways—reducing consumer choice, discouraging third-party software developers from investing in future innovative products, and reducing competition among applications. Mr. Volach and the Blix team have suffered all of these harms. They cannot invest in new software

for MacOS, to serve consumers who use MacOS, if they do not receive fair access to the Mac App Store.

14. Unless consumers have access to Blix on all platforms, including the Mac platform, Blix cannot succeed as a cross-platform messaging solution that services *all* of a company's users. Without the ability to reach MacOS users, Blix cannot serve enterprise users who prefer MacOS, and Blix's success in the marketplace for cross-platform messaging solutions is at grave risk.

15. Apple is not allowed to steal Mr. Volach's ideas, toss Mr. Volach's BlueMail application out of the App Store to prevent competition, and unlawfully leverage Apple's App Store dominance to capture additional market share for its own offerings at the expense of competing technologies. Plaintiff asks this Court to protect its patented inventions, ensure its patented ideas are not used without permission or compensation, and restore access to the App Store marketplace.

NATURE OF THE ACTION

16. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. §§ 1, *et seq.*, and for antitrust violations under the Sherman Act, 15 U.S.C. §§ 1 et seq.

17. Plaintiff filed this lawsuit to stop Defendant's unlawful infringement of Plaintiff's patented inventions, to halt Defendant's unlawful effort to maintain and extend monopolies by illegally blocking competition, and to obtain damages, an injunction, and other relief.

THE PARTIES

18. Plaintiff Blix Inc. is a Delaware corporation with its principal place of business in 101 Hudson Street, Jersey City, New Jersey. Blix is the successor to BlueMail Inc. BVI and BlueMail LLC, the entities that first developed BlueMail.

19. Defendant Apple Inc. is a California corporation headquartered in Cupertino, California. Apple operates retail stores throughout the country, including in this District, where it sells iPhone and iPad devices preloaded with iOS 13 software—including software specially configured for the infringing features of the "Sign In With Apple" service.

JURISDICTION AND VENUE

20. Plaintiff's claims for patent infringement arise under the patent laws of the United States of America, 35 U.S.C. §§ 1 *et. seq*., including 35 U.S.C. § 271. Plaintiff's claims for antitrust violations arise under the Sherman Act, 15 U.S.C. §§ 1 *et seq*., including 15 U.S.C. § 2. This Court has exclusive subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

21. Apple is subject to this Court's personal jurisdiction. Apple has infringed the '284 patent in Delaware by, among other things, engaging in infringing conduct within and directed at or from this District. For example, Apple has purposefully and voluntarily placed its infringing products as described herein into the stream of commerce with the expectation that these infringing products will be used in this District. On information and belief, these infringing products, including devices running iOS 13 such as iPhones and iPads, have been and continue to be used in this District.

22. Apple employs individuals and operates a retail store at 125 Christiana Mall in Newark, Delaware in this District. Upon information and belief, this store sells more infringing iPhones than any other Apple retail location in the country, and sells and/or supports the second-

highest volume of infringing products out of any Apple retail location in the country. *See* "Apple's (AAPL) Delaware Store Claims Title for Selling Most iPhones," available at http://abcnews.go.com/Business/apples-delaware-store-claims-title-selling-iphones/story?id=20650009, a true and correct copy of which is attached as Exhibit 2.

23. Consumers and software developers use the infringing "Sign In With Apple" service with Apple devices throughout the District. Apple has provided the "Sign In With Apple" system, including iOS 13 software containing "Sign In With Apple," to software developers in this District. Apple is also selling devices running iOS 13 to consumers in this District, and pushing software updates to users in this District. As discussed herein Apple has specifically instructed software developers, as well as end-users of Apple devices, to use the infringing features of "Sign In With Apple."

24. On information and belief, "Sign In With Apple" is already live on iOS 13 devices being sold in this District, and being offered as a software update to existing iPhone and iPad devices in this District. On information and belief, users in this District are already using the infringing service—for example, to sign in and communicate with applications such as Kayak and Instacart. On information and belief, infringing aspects of "Sign In With Apple" such as the "Hide Your Email" option are available in, and being used in, this District.

25. Apple has repeatedly availed itself of the jurisdiction of this Court by filing complaints for patent infringement in this District (*see, e.g.*, *Apple Inc. v. HTC Corp. et al*, C.A. No. 11-611-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-544-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-167-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-166-GMS; *Apple Inc. v. Atico Int'l USA Inc. et al*, C.A. No. 8-283-GMS).

26. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391 and 1400 because Apple has a regular and established place of business in this District, is subject to personal jurisdiction in this District, regularly conducts business in this District, and has committed and continues to commit acts of direct and indirect patent infringement in this District.

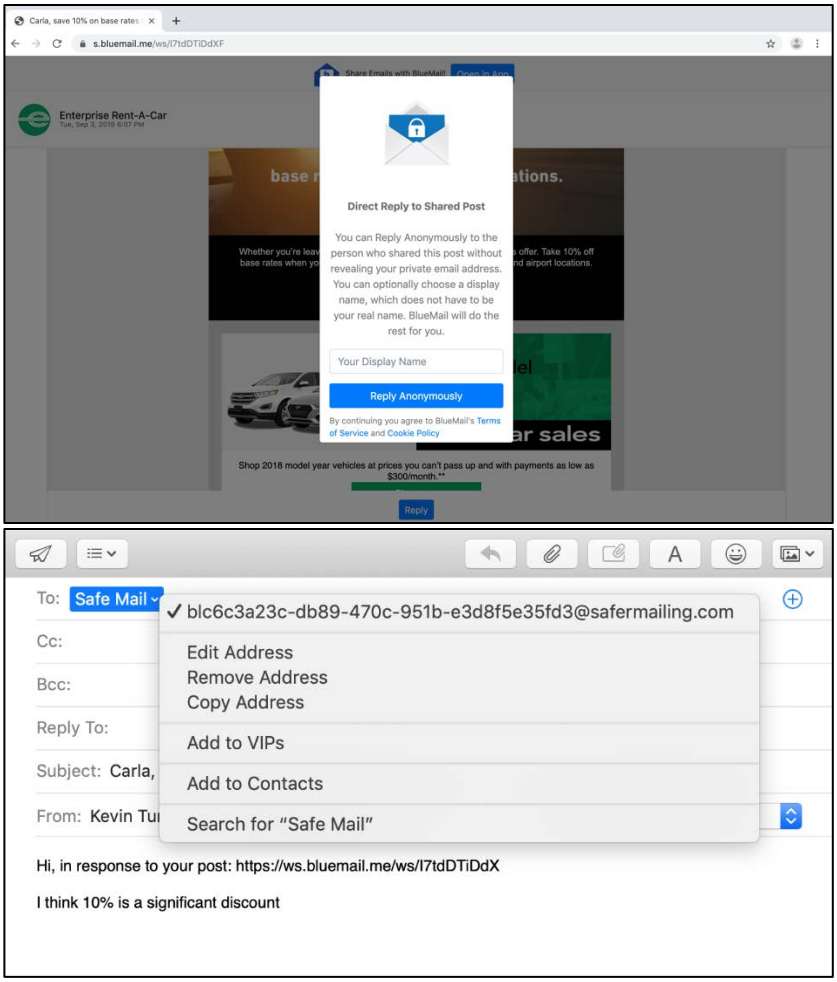
FACTUAL BACKGROUND

Plaintiff's Cutting-Edge Email Services

27. Plaintiff's BlueMail email service is one of the world's leading email clients. BlueMail has repeatedly won awards for its innovative features and its first-in-class user experience.

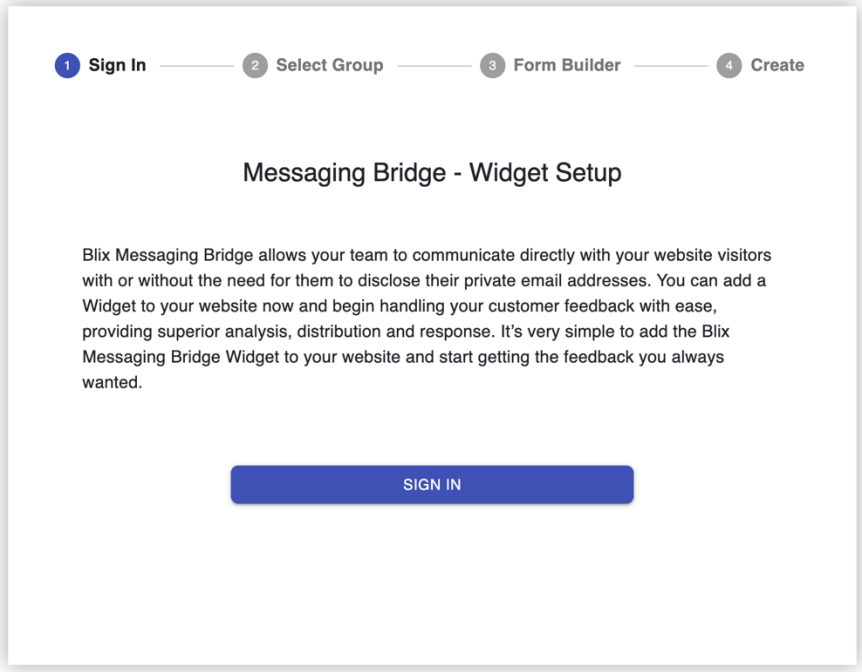
28. BlueMail's success extends to multiple platforms. BlueMail was recently ranked #1 on Android Authority's list of "Top Email Apps For Android."

29. BlueMail's success is driven by its innovative features, including its "Share Email" feature. Using this feature, BlueMail users can post an email to social media platforms, such as Twitter, and can then engage in secure private messaging with others. For example, a business could share an email regarding upcoming discounts on social media, and potential customers could engage in direct communication with the company about that upcoming sale using a manageable *public* interaction address BlueMail automatically provides—so that the potential customer's *private* email address is never revealed to the business.



30. Blix is an evolutionary step forward, and builds on BlueMail's innovative messaging features. Blix is a combined email and messaging platform for companies. It allows users of companies to interact with each other via chat service internally, while interacting with the outside world over email.

31. A major capability of Blix is its Messaging Bridge, allowing a Blix customer to engage visitors to their company website through anonymous interactions with the customer's employees, without revealing their real email addresses.



32. The Blix service has been in active development for more than two years, since March 2017. It was launched in September 2019.

33. Blix's business model is based on selling cross-platform messaging services to companies, to meet all of their messaging needs. The employees of these companies typically run a variety of OS platforms, including MacOS. If Blix is unable to serve Mac OS users, many companies may choose not to work with Blix, and may choose offerings from competing companies instead – for example, Apple.

34. Apple's effort to beat Blix to market, using Blix's own patented technology, substantially threatens Blix's ability to obtain market share—and perhaps to continue operations at all.

The Patent-In-Suit

35. On August 29, 2017, the United States Patent and Trademark Office ("the USPTO") duly and legally issued U.S. Patent No. 9,749,284, titled "Systems and Methods of Controlled Reciprocating Communication."

36. Blix is the owner by assignment of the ’284 patent.

37. A true and accurate copy of the ’284 patent is attached hereto as Exhibit 3.

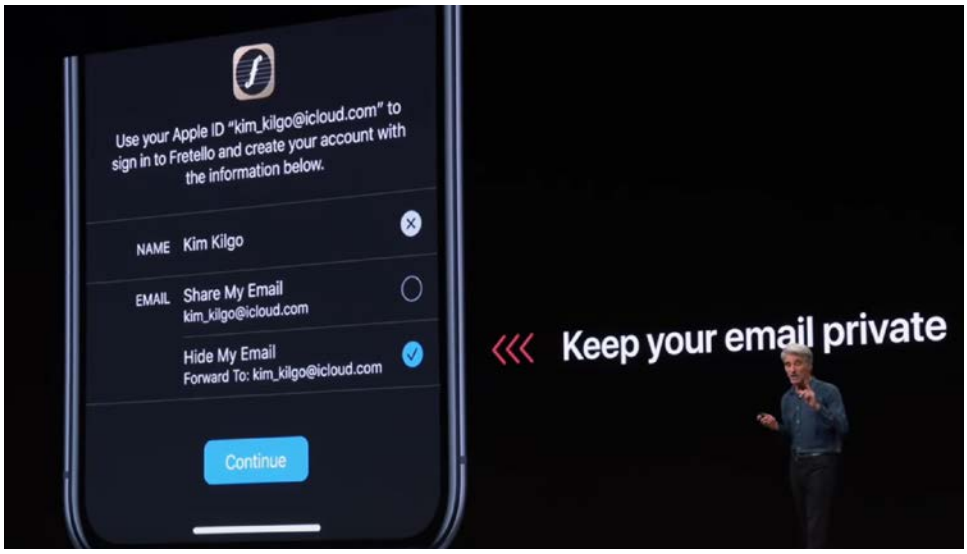
Apple’s Infringement

38. On June 3, 2019, Apple announced its new “Sign In With Apple” service. Apple’s Senior Vice President of Software Engineering Craig Federighi unveiled the service, including its use of public interaction addresses to mask private interaction addresses, to extended and thunderous applause.[1] Mr. Federighi explained that Apple, like many software developers, recognized the growing need for a system to manage interaction addresses and protect privacy; “personal information” too often “gets shared” through online communication, something Apple “wanted to solve” though its new “Sign In With Apple” service.

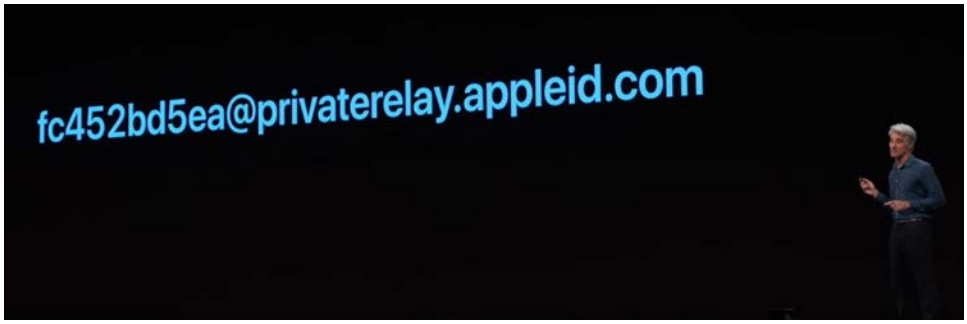
39. Mr. Federighi described the service as “the fast, easy way to sign in without all of the tracking.” This system used a new application programming interface (API) that would permit users to log in to and communicate with applications in a new and more private manner:

[1] A video of the Keynote presentation from Apple’s 2019 Worldwide Developer Conference is available online at https://developer.apple.com/videos/play/wwdc2019/101/. A true and correct excerpt from Apple’s transcript of that presentation, taken from the same website, is attached hereto as Exhibit 4.

"you are authenticated with Face ID on your device, logged in with a new account without revealing any new personal information." Users would be able to log in, but "Keep your email private":

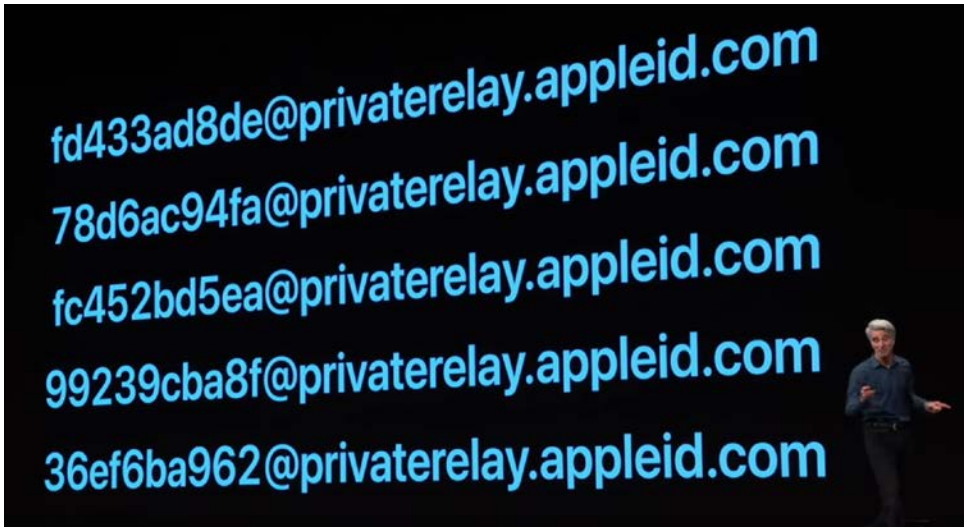


40. As Mr. Federighi explained, the new system worked by assigning public-facing random addresses for the application to interact with the user. These interaction addresses were intended to be easily manageable, relaying communications from public interaction addresses to private interaction addresses using "a unique random address that forwards to your real address."



41. Apple's head of software further explained that this private relay system would assign multiple interaction addresses to facilitate a user's ability to manage interactions with applications; each user would receive a separate interaction address for interactions with specific

developers: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great."



42. Apple's head of software further explained that Apple was offering this system for manageable communications to protect the privacy of users, and to respond to growing demand among users. Giving third parties your electronic addresses information "can be convenient, but it also can come at the cost of your privacy. Your personal information sometimes gets shared behind the scenes and these log ins can be used to track you. We wanted to solve this and many developers do too." But the solution Apple used was not Apple's to use—it was the same system Mr. Volach had already patented several years earlier.

43. In other presentations at Apple's Worldwide Developer Conference in June 2019, Apple continued to encourage software developers to use infringing features of the "Sign In With Apple" service in their software applications. For example, after the keynote address, three Apple engineers gave a separate presentation entitled "Introducing Sign In With Apple."[2]

[2] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/706/. A true and correct excerpt from

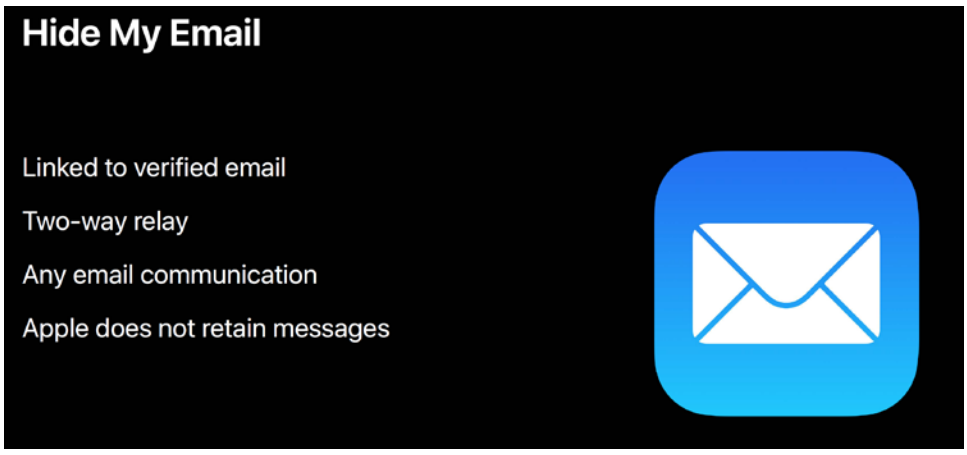
During this hour-long presentation, Apple's engineers gave a large crowd of software developers detailed instructions on how to use infringing "Sign In With Apple" functionality. Those engineers explained that users would often create a host of false, hard-to-manage public interaction addresses to protect their privacy:

44. Apple touted its "Private Relay" service as the solution to this problem, noting that the "Sign In With Apple" system would automatically create email addresses shared between the end-user and the application developer. A developer's emails to this address would be automatically forwarded to the user's private addresses, such that the user could receive email while hiding its email address from the application developer:

Apple's transcript of that presentation, taken from the same website, is attached hereto as Exhibit 5.

Randomly-Assigned Address Is Shared	Private Address Stays Hidden
	

45. Apple touted this "Hide My Email" and "Private Relay" system as a significant step forward in protecting user's privacy, while still enabling easy-to-manage electronic communication. Apple encouraged software developers to use the new API that Apple would be releasing for Apple devices (such as iPhones and iPads running iOS 13), claiming that the API offered an all-encompassing solution for users who desire privacy because its "Hide My Email" features would enable a private "Two-way relay" for "Any email communication" between parties:



46. In another presentation entitled "Designing for Privacy," Apple engineers instructed developers to use infringing features of "Sign In With Apple" in their applications in order to more effectively reach customers concerned with privacy: "we think this is your best

shot at getting your emails in front of your customers."[3] Apple engineers acknowledged that "People can be hesitant to share their real email address" because of privacy problems created by sharing interaction addresses; "We've all seen email lists stolen or resold and then abused by spammers." Apple employees described Apple's new private relay service and "Sign In With Apple" as the best way to facilitate interaction without sharing private interaction addresses:

> Customers can choose to hide their email address, in which case you'll get an address managed by Apple through which we relay your emails to the customer and vice versa…
>
> For each customer, this managed address is different for each developer, so customers are in control of which developers they want to receive email from, and you're in control of who can send emails to the managed address we provide you, since you can whitelist domains or addresses that we'll accept incoming mail from.

47. This presentation by Apple engineers further explained that the code in Apple's new API for "Sign In With Apple" was specifically configured to enable trusted interactions, allowing a software developer to know they are communicating with the intended user even without knowing the user's private interaction address: "With Sign In With Apple, we can leverage on-device intelligence to provide you with one bit that indicates a user is likely real. And that flag is supported on iOS, and we provide it at account creation."

48. Apple's website offers further instructions to developers and end-users on how to utilize infringing aspects of the "Sign In With Apple' service.

49. For example, Apple tells developers that "Sign In With Apple was built from the ground up to give users peace of mind about their privacy," because it offers a secure and private

[3] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/708/. A true and correct excerpt from Apple's transcript of that presentation, taken from the same website, is attached hereto as Exhibit 6.

platform for anonymous messaging: "Apple's private email relay lets users receive email even if they prefer to keep their address private."[4] Apple likewise tells end-users to use the infringing features of "Sign In With Apple." For example: "Sign in with Apple is the fast, easy, and more private way to sign into apps and websites using the Apple ID that you already have."[5]

50. Apple further instructs developers to use Apple's "Private Email Relay Service" to meet user's growing demand for a private and secure communication system that protects their privacy. Apple tells third-party software developers that "Some privacy-conscious users will choose to keep their personal email address private and use Apple's private email relay service when setting up an account. To send email messages through the relay service to the users' personal inboxes, you will need to register your outbound email domains."[6] Apple likewise instructs end-users to use the infringing features of Sign In With Apple: "You can use Hide My Email—Apple's private email relay service—to create and share a unique, random email address that forwards to your personal email. That way you can receive useful messages from the app without sharing your personal email address. Only the registered app or site developer can communicate with you using this email, and you can turn it off at any time."[7]

51. Apple's detailed instructions to software developers instruct them to register up to 10 interaction addresses to use for communications with "Sign In With Apple" users. Specifically, Apple tells developers: "In order to send email messages through the relay service

[4] See "Overview: Sign In With Apple," available online at https://developer.apple.com/sign-in-with-apple/, a true and correct copy of which is attached as Exhibit 7.

[5] See "How to use Sign in with Apple," available online at https://support.apple.com/en-us/HT210318, a true and correct copy of which is attached as Exhibit 14.

[6] See "Make Signing In Easy," available online at https://developer.apple.com/sign-in-with-apple/get-started/, a true and correct copy of which is attached as Exhibit 8.

[7] See Ex. 14.

to the users' personal inboxes, you will need to register your outbound email domains," that "registered domains must create Sender Policy Framework (SPF) DNS TXT records in order to transit Apple's private mail relay," and that a developer "can register up to 10 domains and communication emails" to communicate with "Sign In With Apple" users through the "Private Email Relay Service."[8] Apple likewise gives detailed instructions to end-users on how to use infringing features for anonymous communication[9] and for interaction address management.[10]

52. Apple's "Sign In With Apple" system clearly infringes Mr. Volach's patented techniques in the '284 patent. Yet Apple never sought permission to use these techniques, never acknowledged to developers that these techniques originated with Mr. Volach, and never offered to pay for using these technologies.

Apple's Pattern of Stealing Ideas and Manipulating Markets

53. Apple's misappropriation of Mr. Volach's ideas is part of a long and well-documented pattern of theft by Apple. Steve Jobs, Apple's co-founder, famously admitted "We have always been shameless about stealing great ideas."

54. Apple's practice of stealing great ideas extends to ideas Apple finds in the App Store. As the Washington Post recently noted, Apple frequently takes ideas from third-party applications in the App Store, and uses those ideas to build copycat Apple-branded applications: "Apple plays a dual role in the app economy: provider of access to independent apps and giant

[8] See "Configure Private Email Relay Service," online at https://help.apple.com/developer-account/#/devf822fb8fc, a true and correct copy of which is attached as Exhibit 9.

[9] See "Hide My Email for Sign in with Apple," online at https://support.apple.com/en-us/HT210425#hideemail, a true and correct copy of which is attached as Exhibit 15.

[10] See "Manage the apps you use with Sign in with Apple," online at https://support.apple.com/en-us/HT210426, a true and correct copy of which is attached as Exhibit 16.

competitor to them," and "Developers have come to accept that, without warning, Apple can make their work obsolete by announcing a new app or feature that essentially copies their ideas." Ex. 1.

55. Apple's own former director of App Store review Phillip Shoemaker has admitted, "Apple gets a lot of inspiration from apps that are on the App Store." Mr. Shoemaker further confirmed that Apple collected and analyzed App Store data on third-party applications to decide what ideas Apple would include in its own offerings: "Top Apple executives" could "peek at apps under review," and decisions on which new apps to develop were "made at the top rungs of the company." Mr. Shoemaker would then receive "regular emails from angry app developers, irked that the company had rejected their app or, in some cases, killed their app off by copying them." Ex. 1.

56. This pattern of stealing ideas from the App Store often kills off third-party app developers in the process. As the Washington Post observed: "Apple's past incorporation of functionality included in other third-party apps has often led to their demise." Ex. 1.

57. Apple engages in this pattern of stealing ideas from third-party developers in order to maintain its dominance in the marketplace. Stealing ideas is even more critical to Apple now as sales of the iPhone, its most lucrative product, have slowed. To prove its usefulness to consumers, Apple is offering them more and more services – including innovative services copied from third-party offerings in the App Store.

58. On information and belief, Apple's rejection of BlueMail is part of this same pattern: steal great ideas from the App Store, and then discard what remains of the stolen application.

59. Apple employees have also apparently manipulated App Store results to suppress results from competitors, including BlueMail. As the New York Times recently reported, Apple's manipulation of search results in the App Store has sparked a number of antitrust investigations and complaints: "as Apple has become one of the largest competitors on a platform that it controls, suspicions that the company has been tipping the scales in its own favor are at the heart of antitrust complaints in the United States, Europe and Russia." *See* New York Times, HOW APPLE'S APPS TOPPED RIVALS IN THE APP STORE IT CONTROLS (Sept. 9, 2019) (attached hereto as Ex.10), These concerns are well-founded: "two senior Apple executives acknowledged in a recent interview [with the New York Times] that, for more than a year, the top results of many common searches in the iPhone App Store were packed with the company's own apps," even "when the Apple apps were less relevant and less popular than ones from its competitors."

60. On information and belief, BlueMail suffered from this same suppression in Apple's App Store, inhibiting consumers' ability to discover the application and harming BlueMail's ability to reach consumers and compete with Apple's own offerings.

61. On information and belief, shortly after the New York Times's September 9 story on Apple's manipulation of App Store search results, Apple's ranking algorithms changed, to apparently remove techniques for manipulation and suppression that were under scrutiny. Days after the New York Times story published, BlueMail shot from #143 to #13 on simple keywords such as "email" in the iOS App Store – despite no change in the BlueMail iOS application itself.

Apple's Monopolization: Relevant Markets

62. There are two relevant markets for Plaintiff's antitrust claims: (1) the MacOS App Store Application Aftermarket, and (2) the MacOS Email Client market.

63. MacOS App Store Application Aftermarket. The MacOS App Store is an online marketplace for software programs designed to run on the MacOS operating system.[11] Applications must be designed to run on a specific operating system, such as Windows or MacOS. Once a user makes a selection in the operating system market (*e.g.*, by selecting a Windows computer, a MacOS computer, or some other computer), an aftermarket exists for software applications that will run on that operating system.

64. The existence of competition in the market for operating systems, such as competition between Microsoft's Windows operating system and Apple's MacOS, is irrelevant to relevant market analysis in a Section 2 Sherman Act aftermarket monopolization case, in which the existence or lack of competition in the aftermarket at issue is the only economically meaningful inquiry.

65. Apple encourages all MacOS users to use the App Store as their exclusive source of software applications, claiming it offers unique security benefits.

66. Apple opened its MacOS App Store in January 2011. Apple owns 100% of the MacOS App Store. It staffs the MacOS App Store with Apple employees or agents, and it controls all of the MacOS App Store's sales, revenue collections, business operations, and application approval decisions.

67. Apple maintains 100% control over which applications it will and will not accept into the MacOS App Store. This gives Apple complete control over third-party software developer's access to the MacOS App Store as a distribution channel.

[11] References to "MacOS" herein refer to Apple's operating system for desktop and laptop computers, also referred to at times by Apple in marketing materials as "Mac OS," "Mac OS X," or "OS X." References to the "Mac OS App Store" refer to Apple's "App Store" marketplace for MacOS software applications, first released by Apple in January 2011.

68. Apple's design of the MacOS operating system makes the MacOS App Store its own market – one separate and apart from other potential markets for MacOS software. As explained herein, Apple encourages users to only run software applications if those applications are obtained from the MacOS App Store. A large population of consumers (including all consumers who heed Apple's instructions on security) will not engage with any other distribution channel. Because of Apple's software design choices, the MacOS App Store is not simply a marketplace – it is a software market (or software aftermarket) in and unto itself.

69. The geographic scope of the MacOS App Store Application Aftermarket is national.

70. There are no reasonable substitutes for the MacOS App Store, either for consumers seeking secure software applications or for software developers who wish to reach MacOS users. Indeed, Apple has designed MacOS as an increasingly closed system, including software designed to block applications not downloaded from the MacOS App Store, in order to maintain complete control over the MacOS software aftermarket.

71. For example, Apple's MacOS operating system now includes so-called "Gatekeeper" software designed to block software not downloaded through the MacOS App Store, unless consumers ignore ominous "security warnings" that Apple issues to users, or alter complex security settings on their device. Users are strongly disincentivized from running software that Apple indicates may be harmful for their computer. Thus, software applications downloaded from the Internet, and subject to active security warnings from Apple, are not reasonable substitutes for software applications downloaded through the MacOS App Store, and using the Internet as a channel of direct distribution is not a reasonable substitute for distributing

software through the MacOS App Store, because Apple's own software separates these two channels into separate software markets with separate security implications for users.

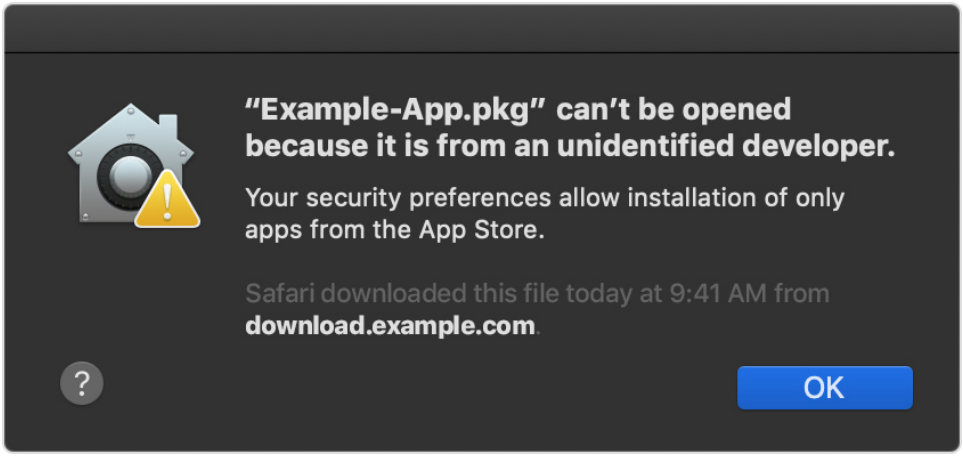
72. Apple documentation confirms that software applications downloaded from the Internet are not a reasonable substitute for software applications downloaded through the MacOS App Store, as Apple actively warns users against downloading and installing applications in this fashion.

73. Apple explicitly tells consumers that downloading applications from the App Store is the only secure way to receive applications, and that Internet downloads are not reasonable substitutes for App Store-approved applications: "The safest place to get apps for your Mac is the App Store… macOS includes a technology called Gatekeeper, that's designed to ensure that only trusted software runs on your Mac… By default, the security and privacy preferences of your Mac are set to allow apps from the App Store and identified developers. For additional security, you can choose to allow only apps from the App Store."[12]

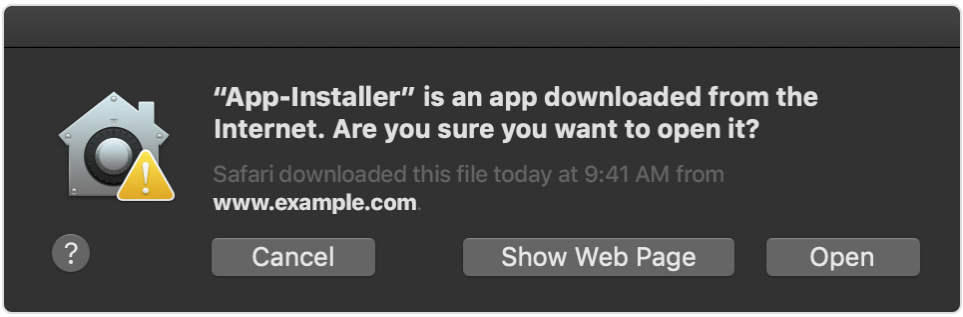
74. Apple's MacOS operating system includes so-called "Gatekeeper" software designed to block software not downloaded through the MacOS App Store, unless consumers affirmatively choose to allow software that Apple ominously warns users may not be safe.

75. Using Apple's recommended settings for "additional security" by "choos[ing] to allow only apps from the App Store" (Ex. 11), a MacOS user is prohibited from downloading and installing applications through any means other than the App Store:

[12] See "Safely open apps on your Mac," online at https://support.apple.com/en-us/HT202491, a true and correct copy of which is attached as Exhibit 11.



76. Even if users ignore Apple's suggested settings for "additional security" (Ex. 11) and opt to allow for installation of software installations received outside the MacOS App Store, Apple further discourages users from installing applications once downloaded, displaying ominous warning messages designed to discourage users from running those applications:



77. Apple's security documentation for users discourages users from accepting software when this warning is displayed: "You may want to look for a later version of the app in the App Store or look for an alternative app."

78. Apple's MacOS security settings for applications, including its Gatekeeper software, are designed to further Apple's strategy to ensure users face significant barriers when attempting to download MacOS software applications through any source other than Apple's MacOS App Store. Apple warns MacOS users that no method of application delivery is a reasonable substitute for the App Store, saying that the MacOS App Store should be sole trusted

source of applications: "The safest place to get apps for your Mac is the App Store… Apple reviews each app in the App Store before it's accepted and signs it to ensure that it hasn't been tampered with or altered." Ex. 11.

79. Given Apple's security warnings and admonishments to consumers, and Apple's Gatekeeper software designed to exclude MacOS applications obtained from sources other than the MacOS App Store, MacOS applications obtained from sources other than the MacOS App Store are not reasonably interchangeable with MacOS App Store downloads.

80. A significant portion of users are unwilling to disregard Apple's security warnings and download and install applications Apple flags as allegedly unsafe, as compared to MacOS App Store downloads.

81. User's desire for security, including for secure MacOS applications, is substantially price-inelastic. Small increases in price for MacOS App Store downloads will not cause reasonable consumers to jeopardize the security of their much more expensive Apple computers, which typically sell for thousands of dollars.

82. The MacOS Email Client Market. An email client is a software application used to send and receive electronic mail. Email clients are local software packages that offer a collection of features designed to facilitate sending, receiving, composing, and organizing email. These local software programs differ from command-line interfaces or from web-based interfaces, which offer a more limited set of features and typically cannot operate locally when a device is not online.

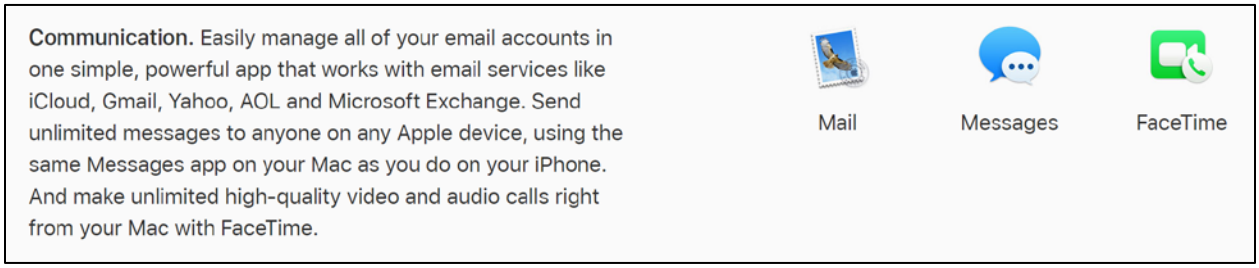
83. Mail clients are software applications designed to run on a specific operating system, such as Windows or MacOS. Email clients designed to run on one operating system (such as Windows) are not substitutes for email clients designed to run on another operating

system (such as MacOS), since a software package designed to execute on one operating system will not execute on another operating system.

84. The geographic scope of the MacOS Email Applications Market is national.

85. The existence of email clients for operating systems other than MacOS is irrelevant to the analysis of the relevant market at issue; software developed for other operating systems is not compatible with MacOS devices, and therefore those applications are not reasonably interchangeable substitutes for MacOS email clients.

86. Apple pre-installs its own email client, Apple Mail, on all MacOS devices. Apple encourages MacOS users to use this "simple, powerful app that works with email services like iCloud, Gmail, Yahoo, AOL and Microsoft Exchange."



See https://www.apple.com/ca/macos/what-is/, a true and correct copy of which is attached as Exhibit 12.

87. By pre-installing Apple Mail on all MacOS devices, Apple has long enjoyed a dominant position in the MacOS Email Client Market. Apple's "Apple Mail" application is installed as the default email client for all 100,000 million MacOS users.

88. Apple's dominance in the MacOS Email Client Market is threatened by competition from innovative entrants, especially BlueMail, that provide a more appealing user experience through a cutting-edge design and a more attractive blend of features to users—

including innovative messaging features not available through Apple Mail. BlueMail's anonymous email features compete directly with Apple's aspirations in this area.

89. The patented private relay features in the '284 patent, employed by BlueMail, are highly attractive to end-users. Apple admitted during its 2019 Worldwide Developers Conference that these anonymous communication features solved a pressing problem Apple and many other software developers wanted to solve, to address end-user concerns and meet market demands: electronic communication "can be convenient, but it also can come at the cost of your privacy. Your personal information sometimes gets shared behind the scenes and these log ins can be used to track you. We wanted to solve this and many developers do too." Ex. 4.

Apple's Monopolization: Eliminating Competition, Including BlueMail

90. On April 6, 2019, BlueMail—which was already wildly popular on mobile operating systems, including iOS and Android—was uploaded to Apple as an application on the MacOS App Store. BlueMail was in Beta testing at that time. This timeframe allowed Apple to better understand BlueMail's targets.

91. BlueMail was submitted for Apple's approval.

92. On May 8, 2019, BlueMail was published to the MacOS App Store and made available for public download in that market.

93. BlueMail was a rapid success in the MacOS App Store. In only a few weeks, BlueMail was one of the top-rated email clients for MacOS.

94. Shortly after Apple witnessed BlueMail's rapid success in the MacOS Email Client Market, Apple suddenly questioned its own decision to publish BlueMail in the MacOS App Store.

95. On May 21, 2019, Apple suddenly and spontaneously claimed that "Upon re-evaluation, we found that your app is not in compliance with the App Store Review Guidelines." Specifically, Apple claimed that BlueMail violated "Guideline 4.3 – Design – Spam" because, according to Apple, "This app duplicates the content and functionality of other apps submitted by you or another developer to the App Store, which is considered a form of spam." Apple threatened to remove BlueMail if a "an update compliant with the App Store Review Guidelines" was not received "within 48 hours."

96. Apple's claim that BlueMail violated "Guideline 4.3" for "Spam," after BlueMail had initially been approved, released, and had grown popular with users, was facially absurd. Apple's "Guideline 4.3" states: "4.3 Spam. Don't create multiple Bundle IDs of the same app. If your app has different versions for specific locations, sports teams, universities, etc., consider submitting a single app and provide the variations using in-app purchase. Also avoid piling on to a category that is already saturated; the App Store has enough fart, burp, flashlight, and Kama Sutra apps, etc. already. Spamming the store may lead to your removal from the Developer Program."

97. Nothing about BlueMail violated Guideline 4.3. BlueMail was and is a high-quality mail client with innovative features and a clean, attractive user interface loved by users—not a "fart" or "burp" application.

98. On May 23, BlueMail engineers uploaded a new version of the application as requested, with a new user interface (UI) design, explaining that "In this release, we have changed the UI and think the app is unique in its capabilities, as well as its design. If you still think the app is too similar to others, can you please elaborate on which apps you find similar, so we can look into it and take action if required."

99. Less than two hours later, on May 23, Apple again rejected BlueMail, claiming that "Your app duplicates the content and functionality of apps currently available on the App Store." Apple declined to identify which supposedly-duplicative applications had triggered the rejection.

100. On June 3, Apple again rejected BlueMail, again claiming that "Your app still duplicates the content and functionality of apps currently available on the App Store."

101. On June 3, BlueMail engineers again asked Apple to explain the basis for this rejection: "Could you please let us know which app or apps do you refer to, as we believe our app is unique and have removed any similar apps from the App Store."

102. On June 4, Apple identified an allegedly-duplicate application: "Your app duplicates the content and functionality of other app submitted by another developer to the App Store, which is considered a form of spam: ***TypeApp***."

103. This June 4 email marked Apple's first reference to TypeApp—a separate mobile application developed by a separate company affiliated with Mr. Volach. TypeApp, unlike BlueMail, targets email service providers, and is customized to the needs of those service providers. For example, TypeApp is customized for Locaweb Servicos de Internet S/A in Brazil, whereas BlueMail has no Brazil-specific customization.

104. Apple's June 4 claim that BlueMail and TypeApp were "duplicates … currently available on the App Store" was false, and a pretext for Apple's anticompetitive decision to eliminate competition from BlueMail's rapid growth. TypeApp for Mac had been voluntarily removed from the MacOS App Store weeks earlier, on May 23, 2019.

105. BlueMail and TypeApp were never duplicate applications—but they certainly could not be "duplicates" on June 4, 2019 that were "currently available on the App Store" when TypeApp for Mac had already been voluntarily removed weeks earlier.

106. On June 5, BlueMail engineers explained this to Apple, noting that "We just checked again the Mac App Store and TypeApp was indeed removed (Developer rejected) from the store. This makes us a unique app. Can you please approve our latest version, or should we upload a new version?"

107. On June 5, even after the false nature of its pretextual justification for the rejection had been pointed out, Apple refused to withdraw its rejection, without explanation or apology. Apple simply stated that "After further review and consideration we have found that your application is still not in compliance with our guidelines."

108. On June 7, 2019 at 3:15am EST, days after Apple announced its infringing "Sign In With Apple" service that mimicked certain BlueMail functionality, Apple finally removed BlueMail from the MacOS App Store, without any further explanation for its conclusory June 5 claim that BlueMail was "not in compliance with our guidelines."

109. Apple removed BlueMail from the MacOS App Store, and, based on Apple's statements, on information and belief removed other unnamed other "duplicate" applications with the same "content and functionality" as the BlueMail mail client. This pattern of removing MacOS mail clients shielded the Apple Mail email application from competition.

110. On information and belief, Apple's removal of BlueMail under Guideline 4.3 was pretextual. At all relevant times Apple knew BlueMail was not spam, knew that BlueMail did not violate Guideline 4.3, and did not in good faith believe BlueMail was duplicative of other

applications. Apple's vague rejection was part of Apple's scheme to remove competition from the App Store.

111. By reducing competition in the MacOS Email Client Market, Apple harmed innovation. MacOS software developers have no incentives to create new software with new features and new functionality if they cannot recoup their investments in research and development by actually distributing their software and reaching users. Apple's decision to block access to the MacOS App Store based on vague claims of duplicate "features and content" discourages entry in the MacOS email client market, and disincentivizes the creation of competing software products in that market.

112. According to Apple's announcements, "Sign In With Apple" will be available on all platforms, accessible for everyone on the Internet, including Windows and Android. Apple has realized the crucial importance of cross-platform availability and has specifically advertised cross-platform availability of the "Sign In With Apple" service: "Sign In with Apple is cross-platform. The API is available on all Apple platforms: iOS, MacOS, WatchOS, tvOS. The sign-in experience is tailored on each platform for ease of use. The JavaScript API enables you to use Sign In with Apple on the web as well as other platforms like Windows or Android."[13]

113. "Sign In With Apple"—and particularly, its infringing features for anonymous communication—appears to be a critical component of Apple's plans for the future of messaging. Apple's own CEO explained that Apple is betting heavily on this feature and its anonymous communication features, explaining in public comments (which were made just

[13] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/706/. A true and correct excerpt from Apple's transcript of that presentation, taken from the same website, is attached hereto as Exhibit 5.

before Apple dropped BlueMail for Mac from the App Store) on June 3rd, 2019: "We are pushing forward and I hope that everyone that wants to not be surveilled across the Internet, I hope they use our Sign In."[14]

COUNT I

INFRINGEMENT OF THE '284 PATENT

114. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

115. As explained herein, and on information and belief, Apple has directly infringed, and continues to directly infringe, at least claims 1-5, 7-10, 12-13, 17-18, 21-22, 26-30, 33-34, and 36-37 of the '284 patent by making, using, offering for sale, selling, and/or importing into the United States the infringing "Sign In With Apple" system, including iOS devices with an API specifically configured to perform infringing operations, and has contributed to and/or induced infringement of the '284 patent by others, including software developers and end-users.

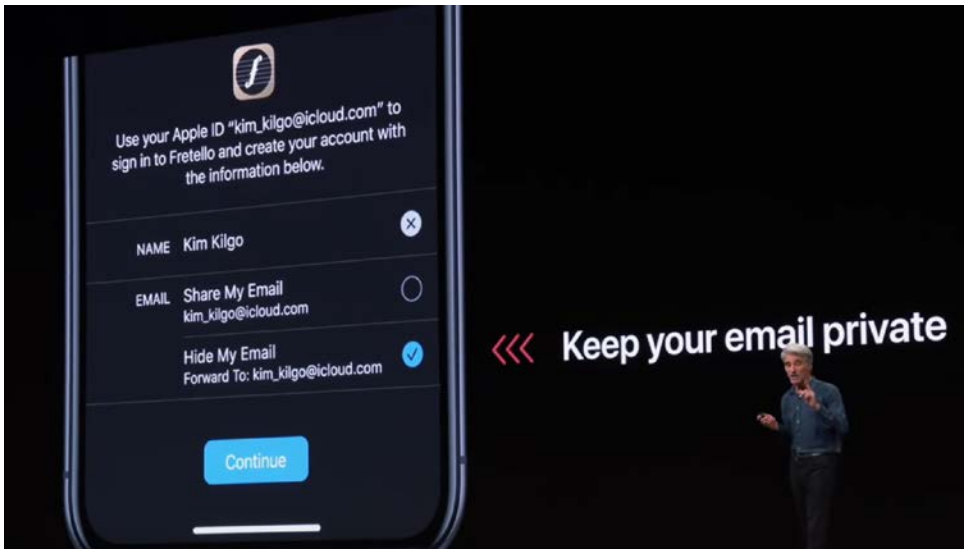
116. For example, and without limitation, on information and belief the "Sign In With Apple" system meets every limitation of at least claims 17 and 26 of the '284 patent, and Apple's making, using, offering for sale, selling, and/or importing the "Sign In With Apple" system, including iOS devices running iOS 13, and Apple's distribution of iOS 13 to such devices, directly infringes claim 1 of the '284 patent under 35 U.S.C. § 271(a).

117. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, perform a method of controlled pre-interaction between a first party and at least one second party. For example, a first party, such as an end-user of an

[14] Tim Cook in an interview with Norah O'Donnell to CBS News on June 3, 2019, https://www.cbsnews.com/video/tim-cook-on-immigration-tariffs-and-spending-too-much-time-on-our-phones/, attached hereto as Exhibit 13.

Apple device, and at least one second party, such as an application developer, can perform controlled pre-interaction, such as operations performed prior to communications between the end-user and the application developer, to ensure that subsequent communications via private relay will not inform the application developer of the end user's private email address. Apple documentation confirms "Apple's private email relay lets users receive email even if they prefer to keep their address private." Ex. 7 Moreover, "Sign In With Apple" will also perform controlled pre-interaction operations for at least login and authentication purposes; when using the "Sign In With Apple" system, "you are authenticated with Face ID on your device, logged in with a new account without revealing any new personal information." Ex. 4.

118. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, provide at least one private interaction address of said first party. For example, Apple presents to a first party, such as an end-user of an Apple device, at least one private interaction address of that end-user, such as an email address. Apple provides this email address to users upon sign-in via an interface asking users if they wish to "Share My Email" or "Hide My Email," as shown below:



See also Ex. 4.

119. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, defines at least one manageable public interaction address for said first party. For example, Apple defines a random email address for an end-user who selects the "Hide My Email" option. *See* Ex. 4; Ex. 5. This email address is designed to be manageable, and can be disabled at any time by an end-user: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great." Ex. 4.

120. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, forms a record, wherein said manageable public interaction address is associated with said private interaction address for said first party. For example, when the random email address receives an email from a specific application developer, Apple forwards that email to the end-user's private email address. On information and belief, Apple forwards these messages using records that associate the random email address with the user's private email address.

121. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, generates a reverse list, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party. For example, the interaction address of an application developer is associated with an end-user's random address when the "Hide My Email" option is selected. Apple associates each random email address with one specific application developer: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great." Ex. 4.

122. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, performs at least one pre-interaction act, said pre-interaction act comprises accessing said reverse list, and identifying said interaction address of said second party in said reverse list. For example, on information and belief, Apple accesses a reverse list to identify the email address of an application developer before forwarding email to that application developer via its private relay service.

123. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, determines that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party. For example, on information and belief, the "Sign In With Apple" private relay system determines that a randomly-generated email address associated with an end-user is also associated with an application developer, at least in order to ensure that communications to the randomly-generated email address are only forwarded to the end-user if they are received from the application developer.

124. The "Sign In With Apple" system, including Apple devices specifically configured to work with that system, performs a method wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address. For example, on information and belief, Apple's "Sign In With Apple" service allows application developers to register email addresses that are obtainable from third parties and external services providers, including obtainable from Apple. Moreover, on information and belief, at least one reverse list entry in Apple's "Sign In With Apple" system is formed by synchronizing an application developer's registered email

address with the randomly-assigned email address assigned for an end-user's communications with that application developer.

125. Apple's own use of Apple devices specifically configured to use the "Sign In With Apple" system and set that system in motion, including without limitation use during testing of devices such as iPhones and iPads running iOS 13, directly infringes claim 17. These infringing uses include, without limitation, Apple's testing in the United States of said devices, as well as Apple's demonstrations of the infringing method, including demonstrations to application developers, media, end-users, and to potential customers—including, on information and belief, demonstrations by Apple Store employees at the Apple Store in this district.

126. Apple's making, using, offering for sale, selling, and/or importing devices specifically configured to use the "Sign In With Apple" system and set that system in motion, including without limitation devices (such as iPhones and iPads) running iOS 13, infringes claim 26. These devices contain non-transitory computer readable media having computer-executable instructions that, when executed, perform a method of controlled reciprocating communication, as explained above with respect to claim 17.

127. Thus, the use of Apple's "Sign In With Apple" system meets every limitation of at least claim 17. Moreover, the sale of iOS devices specifically configured to use and place that system in motion infringe at least claim 26. Apple directly infringes at least those claims by offering the "Sign In With Apple" system, and devices specifically configured to place that system in motion, in violation of 35 U.S.C. § 271(a).

128. Apple has also indirectly infringed, and continues to indirectly infringe, the claims of the '284 patent by inducing infringement pursuant to 35 U.S.C. § 271(b) and/or contributing to infringement pursuant to 35 U.S.C. § 271(c).

129. On information and belief, in violation of 35 U.S.C. § 271(b), Apple specifically intended to induce infringement of the ’284 patent by application developers and end-users of Apple devices, and had knowledge that the inducing acts would cause infringement, or was willfully blind to the possibility that their inducing acts would cause infringement.

130. On information and belief, Apple knew of the ’284 patent since at least as early as June 2019, when Apple removed the competing BlueMail product from the App Store only days after announcing its infringing “Sign In With Apple” system. Apple has also known of the ‘284 patent, and of its infringement of that patent, at least since filing and service of this complaint.

131. On information and belief, Apple’s customers directly infringe the ’284 patent. For example, when and end-user uses the “Sign In With Apple” system in the manner intended by Apple, including for the purposes of communicating via private relay between an end-user and an application developer by way of a randomly-assigned unique email address, those activities infringe at least claim 17 of the ’284 patent. Similarly, when Apple software developers use the “Sign In With Apple” system in this manner for reciprocal communications with end-users, those activities likewise infringe at least claim 17 of the ‘284 patent.

132. On information and belief, Apple specifically intends for end-users and application developers to directly infringe the ’284 patent. Apple encourages infringement by instructing end-users and application developers by way of product support, developer documentation, and live instructional presentations that instruct users and applications developers on how to use the infringing “Sign In With Apple” system. *See, e.g.*, Ex. 4-9, 14-16.

133. On information and belief, despite Apple’s knowledge of the ’284 patent and knowledge that end-users and application developers will necessarily infringe the ’284 patent

when using the "Sign In With Apple" system as instructed, Apple continues to encourage infringement.

134. Apple actively encourages application developers to create applications that use the "Sign In With Apple" service, as described herein and in Exhibits 4-9 hereto.

135. Apple's "Sign In With Apple" application programming interface (API) is specifically designed to perform the infringing functionality described herein. This API has no substantial non-infringing uses; it is designed to carry out the infringing functionality that forms the basis for Plaintiff's patent infringement claims.

136. Defendant also contributes to infringement of the '284 patent by Apple's end-users and application developers in violation of 35 U.S.C. §271(c). On information and belief, Apple knew of the '284 patent since at least as early as June 2019, when it chose to eliminate an embodiment of that patent from the App Store only days after announcing its competing and infringing "Sign In With Apple" system. On information and belief, Apple offers to sell and sells within the United States devices specifically configured to operate with the "Sign In With Apple" system knowing that they constitute a material part of the claimed inventions, knowing that the "Sign In With Apple" API is especially made or especially adapted for use in infringing the '284 patent, and knowing that the "Sign In With Apple" system is not a staple article or commodity of commerce suitable for substantial non-infringing use.

137. Apple has committed and continues to commit all of the above acts of infringement without license or authorization.

138. As a result of Apple's infringement of the '284 patent, Plaintiff has suffered damages and will continue to suffer damages.

139. On information and belief, Apple's infringement of the '284 patent has been and continues to be willful. Apple has had knowledge of BlueMail and, on information and belief, has had knowledge of the '284 patent, since Apple decide to remove the BlueMail embodiment from the App Store days after announcing its competing and infringing "Sign In With Apple" service. On information and belief, Apple copied the '284 patent's innovative disclosures, including features used in the BlueMail software, before throwing the BlueMail software application out of Apple's App Store marketplace. Apple offered a competing system for private communication knowing the risk of infringement and/or in view of a risk of infringement that was sufficiently obvious that it should have been known to Apple. Despite this risk, Apple has deliberately continued to infringe in a wanton, malicious, and egregious manner, with reckless disregard for Plaintiff's patent rights. Defendant's infringing actions have been and continue to be consciously wrongful, entitling Plaintiff to increased damages under 35 U.S.C. § 284.

140. Under 35 U.S.C. § 283, Plaintiff is entitled to injunctive relief precluding further infringement. Apple's wrongful conduct has caused and will continue to cause Plaintiff to suffer irreparable harm resulting from the loss of its lawful patent right to exclude others from making, using, selling, offering to sell, and/or importing Plaintiff's patented inventions. On information and belief, Apple will continue to infringe the '284 patent unless enjoined by this Court.

COUNT II

ILLEGAL MONOPOLOZATION UNDER 15 U.S.C. § 2

141. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

142. Apple has monopoly power in the MacOS Email Client Market.

143. Apple's ability to exclude competition in the MacOS Email Client Market is direct evidence of its monopoly power.

144. Apple's own Apple Mail email client is pre-installed on 100% of end-user's MacOS machines.

145. Apple's complete control over the MacOS App Store, and consequently the MacOS App Store Application Aftermarket, impose a significant barrier to entry in the market for MacOS email clients.

146. Apple illegally leveraged its monopoly power over MacOS application distribution in order to maintain and extend its monopoly position in the market for MacOS email clients.

147. Apple purports to have the authority to remove any application that allegedly "duplicates" another application's features—for example, the features of Apple's own Apple Mail email client, which is already present on all MacOS computers by default – and Apple has used this authority to remove competition in the MacOS Email Client Market, including competition from BlueMail and other unnamed email clients Apple alleged were "duplicates."

148. Apple willfully maintained its monopoly power in the MacOS Email Client Market through its anticompetitive conduct described above. In so doing, Apple inflicted substantial antitrust injury on Plaintiff in violation of the Sherman Act, § 2.

149. No competitors can enter the MacOS Email Client Market and effectively compete with Apple without access to the MacOS App Store Application Aftermarket, which Apple created to erect significant barriers to entry in the MacOS application aftermarket.

150. Apple abused its market power in the MacOS App Store Application Aftermarket (a market Apple created, separate from Internet distribution, through its Gatekeeper software and

other software intended to exclude applications that were not Apple-approved) to protect and extend its monopoly in a separate market—the market for MacOS email clients.

151. Any purported procompetitive justification Apple might raise to rationalize its anticompetitive conduct fails because it is pretextual. Apple's own correspondence with BlueMail (and its pretextual claims of "duplication" with TypeApp, an app that was no longer available on the App Store) demonstrates that Apple's stated reasons for BlueMail's removal were pretextual.

152. But for Apple's unjustified actions, BlueMail would have continued its ascent as a leading MacOS email client.

153. Apple removed the threat of competition from BlueMail, and precluded BlueMail from reaching a larger user base and obtaining user loyalty in the market, that BlueMail would rightfully have earned through open competition.

154. Apple's removal of BlueMail from the App Store, shortly after stealing BlueMail's innovative features for easy-to-use, readily manageable anonymous communications, was part of a pattern of anticompetitive behavior. Apple leverages its App Store to identify great ideas, misappropriate those ideas, and then eject competing applications from the App Store—sometimes driving software developers out of business.

155. Consumers and software developers, including Blix, suffer from Apple's pattern of stealing great ideas Apple sees in the App Store. Apple's pattern of stealing ideas from the App Store reduces consumer choice, discourages third-party software developers from investing in future innovative products, and reduces competition among applications.

156. Apple has engaged in illegal monopolization of the MacOS Email Client Market in violation of § 2 of the Sherman Act and is liable to Plaintiff for damages in an amount to be determined at trial.

JURY DEMAND

157. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that judgment be entered in favor of Plaintiff and against Apple as follows:

a. A judgment that the ’284 Patent is directly and indirectly infringed by Apple’s offers to sell, sales of, and uses of the “Sign In With Apple” system within the United States, or importation into the United States of products, including without limitation iOS products and other products using the “Sign In With Apple” API, that practice one or more of the inventions claimed in the ’284 Patent;

b. A judgment that Apple’s conduct, as alleged, is unlawful under § 2 of the Sherman Act;

c. An order preliminary and permanently enjoining Apple, its affiliates and subsidiaries, and each of its officers, agents, and employees and those acting in privity or concert with them, from making, using, offering to sell, selling, importing products or systems claimed in any of the claims of the ’284 Patent, and from causing or encouraging others to use, sell, offer for sale, or import products or systems that infringe any claim of the ’284 Patent, until after the

expiration date of the ’284 Patent, including any extensions and/or additional periods of exclusivity to which Plaintiff is or may become entitled;

d. A permanent injunction prohibiting Apple from further illegal monopolization and attempted monopolization of the MacOS Email Client Market;

e. An award of damages under 35 U.S.C. § 284 in an amount sufficient to compensate Plaintiff for its damages arising from Apple’s infringement, including, but not limited to, lost profits and/or a reasonable royalty, together with pre-judgment and post-judgment interest, and costs;

f. An award of damages adequate to compensate BlueMail for Apple’s illegal monopolization of the MacOS Email Client Market, based on lost sales, lost profits, price erosion, loss of market share, or any other theory the Court finds applicable, together with prejudgment interest from the date the illegal monopolization began;

g. An order awarding treble damages for willful infringement by Apple, pursuant to 35 U.S.C. 284;

h. An order awarding treble damages under 15 U.S.C. § 15;

i. An accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court’s decision regarding the imposition of a permanent injunction;

j. A judgment declaring that this case is exceptional and awarding Plaintiff its reasonable costs and attorneys’ fees pursuant to 35 U.S.C. § 285;

k. An award to Plaintiff of its reasonable attorney’s fees and costs under 15 U.S.C. § 15; and

l. Such other relief as this Court or a jury may deem proper and just under the circumstances.

/s/ David M. Fry

John W. Shaw (No. 3362)
Karen E. Keller (No. 4489)
David M. Fry (No. 5486)
SHAW KELLER LLP
I.M. Pei Building
1105 North Market Street, 12th Floor
Wilmington, DE 19801
(302) 298-0700
jshaw@shawkeller.com
kkeller@shawkeller.com
dfry@shawkeller.com
Attorneys for Plaintiff

OF COUNSEL:
Steven C. Cherny
Patrick D. Curran
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Ave., 22nd Floor
New York, New York 10010
(212) 849-7000

Adam Wolfson
QUINN EMANUEL URQUHART & SULLIVAN, LLP
865 S Figueroa Street
Los Angeles, CA 90017
(213) 443-3000

Dated: October 4, 2019